EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

EPIC GAMES, INC., Plaintiff v. APPLE INC., Defendant	)	CASE NO.: 4:20-cv-05640-YGR

REBUTTAL EXPERT REPORT OF AVIEL D. RUBIN, PH.D.

March 15, 2021

VI. SUMMARY OF PRINCIPAL CONCLUSIONS

A. Apple's brand and reputation are rooted in customer security, privacy, and reliability; commitment to that brand underlies every aspect of Apple's business, including the iOS mobile operating system and the App Store.

B. There are multiple ways of distributing apps on iOS. Public distribution such as distribution via the App Store undergoes a review process that is both automated and manual. There are significant security advantages attributable to the use of both automatic and manual review of apps distributed via the App Store.

C. The App Store on iOS provides consumers and developers with a safer app distribution marketplace for mobile phone devices relative to other mobile app marketplaces.

D. The security, privacy, and reliability of apps distributed via the App Store are superior to those of other mobile app distribution marketplaces, particularly that of Android. Apps distributed via the App Store are trusted to be safer and more reliable than apps distributed via Android marketplaces.

E. The consumer expectations regarding security, privacy and reliability for mobile devices are significantly different from those expectations for desktop and laptop computers. Apple has reasonably made the conscious decision to design its iOS devices to meet these differing consumer expectations, resulting in a lower frequency of cyberattacks against consumers and app developers.

F. Using Apple's unified In App Payment ("IAP") mechanism is highly beneficial to user security and privacy, as it ensures payment record traceability and safeguards user data. Apple's IAP system also contributes considerably to Apple's ability to identify fraud.

G. Both Drs. Mickens and Lee take a narrow and limited approach to security that does not accurately reflect the goals of the iOS ecosystem nor its operations. Both experts cherry-pick datapoints and assume inaccurate facts to support their opinions, including, for example, inaccurately characterizing (1) on-device security mechanisms; (2) aspects of Apple's Developer Enterprise Program; (3) the translatability of macOS processes to iOS; and (4) users' ability to detect risky apps. They additionally overlook other aspects of Apple's App Store review that enhances the trustworthiness and safety of the platform.

H. Drs. Mickens and Lee propose various hypothetical security recommendations that would reduce the overall security and trustworthiness of the iOS platform. For example, many third-party app stores will lack the resources and incentives to provide security, privacy, and trustworthiness measures comparable to those of the App Store. More lenient measures could be taken advantage of by malicious actors, which would erode Apple's ability to curate apps on the iOS platform to best maintain a safe and trustworthy experience for its users and lead to an overall degradation of trustworthiness, security, and stability of the iOS platform. This can be demonstrated by, for example, a case study of the various security and privacy issues that have arisen as a result of the proliferation of third-party Android app distribution stores in China.

I. The risk of compromise of the security, privacy, and trustworthiness of the iOS platform would be heightened by the imposition of various potential prohibitions upon Apple. Various of Drs. Mickens and Lee's proposals appear to assume that Apple would maintain the ability to warn users about security risks associated with third-party stores or push out iOS updates, for example; if Apple were prevented from taking such security actions, the opinions of Epic's experts would be further undermined.